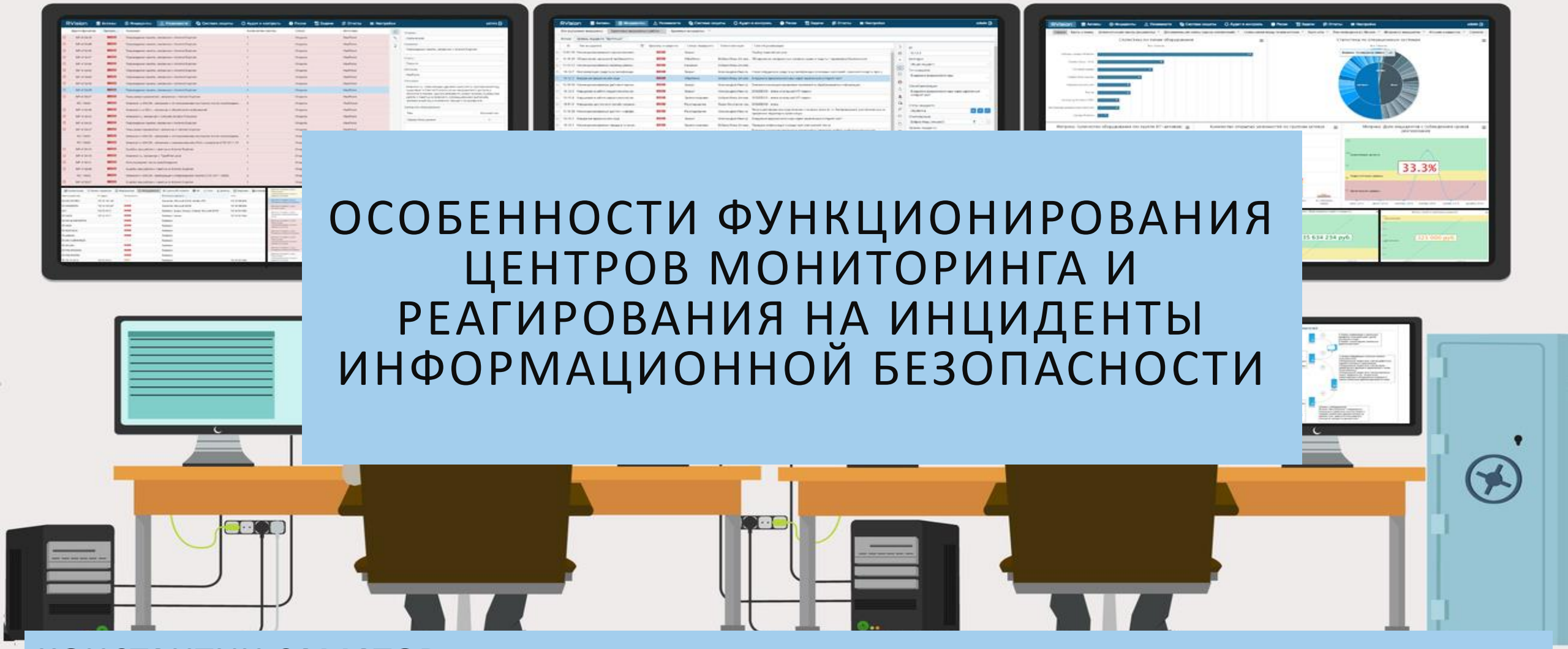


ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ ЦЕНТРОВ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОНСТАНТИН САМАТОВ

Директор Центра информационной безопасности Института менеджмента и информационных технологий
Уральского государственного экономического университета
Руководитель комитета по безопасности КИИ, член Правления Ассоциации руководителей служб информационной безопасности

ЧТО ТАКОЕ SOC?

Security Operation Center (SOC) – Центр мониторинга и реагирования на инциденты информационной безопасности

Возможности SOC

Эффективное обнаружение и предотвращение атак, а также устранение причин возникновения инцидентов

Объективная картина состояния защищенности компании. Повышение уровня устойчивости к атакам

Снижение риска проникновения в инфраструктуру

Своевременное оповещение о возникновении угроз для деловых-процессов

Уменьшение времени реакции на инциденты благодаря готовым сценариям реагирования и использования средств автоматизации

Рекомендации по корректировке защитных мер, подготовка критериев, аналитическая работа

Выявление, регистрация, учет инцидентов, подготовка отчетности

Минимизация последствий, ущерба, затрат на локализацию и устранение инцидента

ВАРИАНТЫ ПОСТРОЕНИЯ SOC

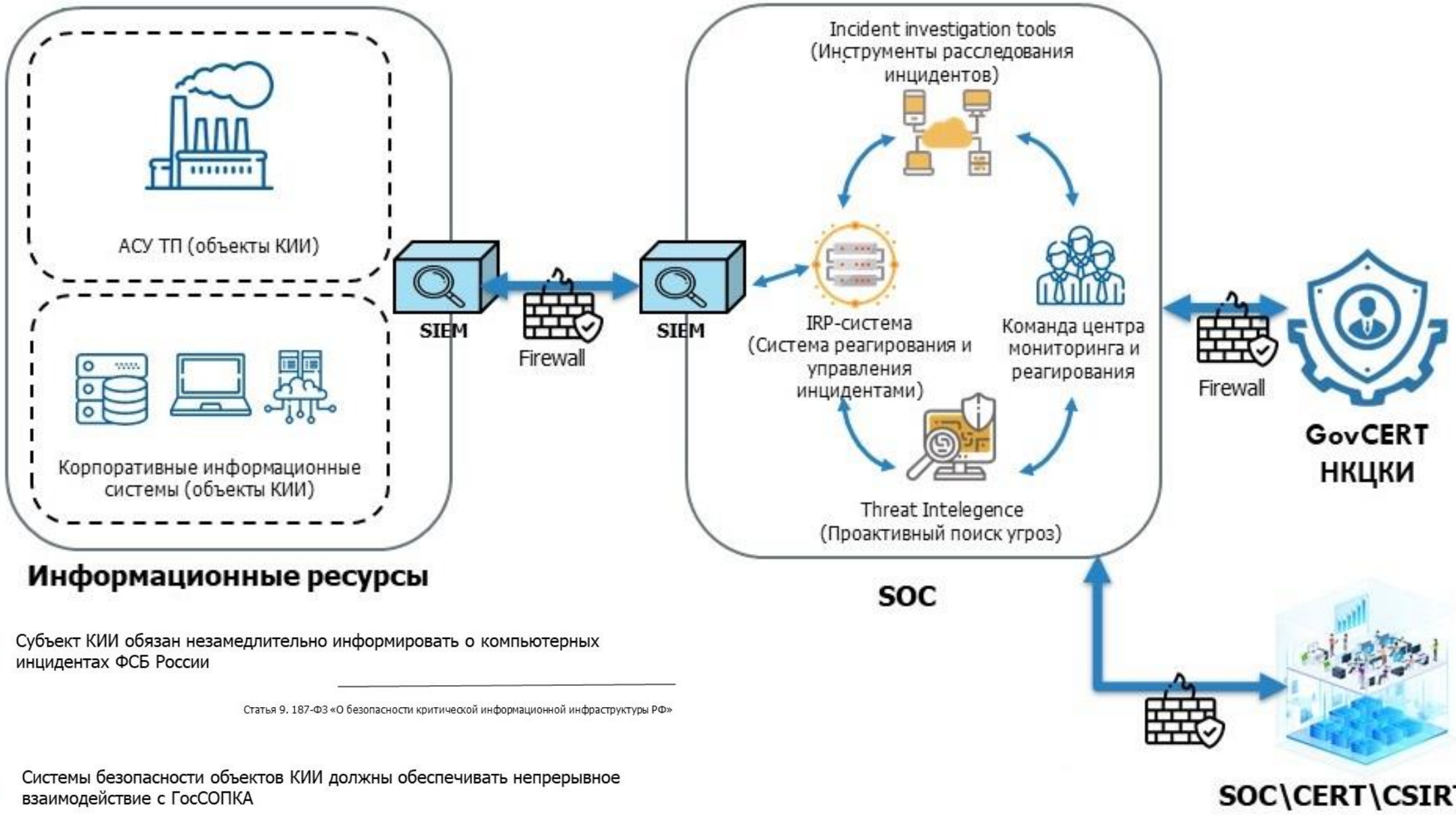
Аутсорсинг SOC

- «Быстрый старт»
- Сформированный штат профессиональных работников, реализующих функции SOC
- Отсутствие затрат на постоянное обучение и повышение уровня компетенции штата профессиональных работников
- Выстроенные управленческие процессы, процессы реагирования и взаимодействия
- Сложность контроля подрядчика, ответственность перед государством несет Субъект КИИ, а не подрядчик
- Утеря компетенций в случае отказа от подрядчика

Собственный SOC

- Создание единого Центра компетенций по обеспечению безопасности объектов КИИ и реагированию на инциденты ИБ
- Оптимизация процессов управления ИБ и штата сотрудников, задействованных в процессах обеспечения безопасности КИИ и реализации функций SOC
- Необходимость оформления лицензии ФСТЭК России на деятельность по мониторингу событий ИБ для выделенного подразделения (организации) при подключении сторонних организаций (в т.ч. дочерних и зависимых обществ)
- Высокие затраты на формирование квалифицированного штата работников, обеспечивающих функционирование SOC, на внедрение технических средств, на процессное обеспечение и дальнейшее поддержание уровня компетенций
- Долговременность создания сервиса SOC

SOC И ГОССОПКА?



Субъект КИИ обязан незамедлительно информировать о компьютерных инцидентах ФСБ России

Статья 9. 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

Системы безопасности объектов КИИ должны обеспечивать непрерывное взаимодействие с ГосСОПКА

Статья 10. 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

СТРУКТУРА ГОССОПКА

Проблемные вопросы взаимодействия с ГосСОПКА

Какую информацию нужно передавать в ГосСОПКА субъекту КИИ?

Обязательно ли подключение к ГосСОПКА?

Нужно ли получать лицензии для подключения к ГосСОПКА?

Когда нужно создавать SOC: до создания СБ ЗОКИИ, после, в процессе?

Обязательно ли создавать (SOC) КЦ субъекту КИИ?

Как быть с аутсорсингом если нет коммерческих центров в структуре ГосСОПКА?

Спасибо за внимание!